UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/528,456	03/17/2000	Martin Kienzle	YOR000028US1	4380

46069 7590 02/08/2005

F. CHAU & ASSOCIATES, LLC
130 WOODBURY ROAD
WOODBURY, NY 11797

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/528,456	**Applicant(s)** KIENZLE ET AL.	
	Examiner Taghi T. Arani	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 November 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *1/8/04*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claims 1-34 are pending in this Office Action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over REITMEIER et al. to US 2002/0003881 in view of York-Smith to U.S. Patent 5, 548, 648.

Referring to claim 1, 20, and 33, REITMEIER et al. teach a system and method comprising a server [Page 1, paragraph 0017, Fig.1, information provider equipment, 105-140] coupled to a transmission link [Figure 1, distribution channels, 145A and 145B] for providing a data stream to at least one client [see Figure 5, subscriber equipment, 150-175] over the transmission link [Figure 1, distribution channels, 145A and 145B], the data stream being segmented into units [page 2, paragraph 0023, Fig 1, segmentation module 110], the server including a scrambler [Fig. 1, information stream encryption module, 135] for encrypting at least one first unit using an encryption key [page 3, paragraph 0031].

REITMEIER et al. do not teach a system or method of a server comprising a steganographic unit for embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by the client to determine the encryption key and decipher the data stream.

However, York-Smith teaches does teach a system and method of a server comprising a steganographic unit for embedding the encryption key into at least one second unit. [York-Smith, see Fig. 1, CB, Fig. 3, Cb1, ..., CBn), col. 3, lines 25-54].

It would have been obvious to one of ordinary skill in the art at the time
The invention was made to modify REITMEIER et al. to include the steganographic teachings of York-Smith. Namely, inserting a steganographic unit in the " information provider equipment" 105-140 of Figure 1[see REITMEIER et al.]. One of ordinary skill in the art would have been motivated to modify REITMEIER et al. as above for the purpose of improving the security of the encrypted data to be transmitted over an unsecured communication line.

Referring to claim 2, REITMEIER et al. as modified by York-Smith teach a steganographic unit employing a steganographic masking algorithm [col. 4, lines 46-56] of York-Smith].

Referring to claims 3 and 21, REITMEIER et al. teach the system as recited in claims 1 and 20, wherein the data stream includes a transmission order which alternates between first units and second units [REITMEIER et al., page 3, paragraph 0034].

Referring to claim 4, REITMEIER et al. as modified by York-Smith teach steganographic unit encrypts the at least one second unit [col. 5, lines 15-16 of York-Smith].

Referring to claims 5 and 23, REITMEIER et al. as modified by York-Smith teach at least one first unit and the at least one second unit are encrypted and
each carries a portion of the encryption key [col. 3, line 65 through col. 4, lines 22].

Referring to claims 6 and 24, REITMEIER et al. teach a transmission link including the Internet [page 3, paragraph 0033].

Referring to claims 7 and 25, REITMEIER et al. teach at least one of the client and the server include a memory storage device [page 3, paragraph 0035].

Referring to claims 8, 14, 26, and 34, REITMEIER et al. teach a system and method comprising a client system coupled to a transmission link for receiving a data stream to at least one server over the transmission link, the data stream being segmented into units, the client system including a descrambler for descrambling at least one second unit which was encrypted in accordance with the encryption key before transmission from the server [col. 3, paragraphs 0035-0036, see also Fig. 1].

REITMEIER et al. teach do not teach a system or method of a client comprising:

a key extractor for extracting an encryption key steganographically hidden in at least one first unit in the data stream received from the server such that steganographic information is needed by the client to determine the encryption key; and

a decoder coupled to the key extractor and the descrambler for reassembling the data stream such that all of the units of the data stream are needed to decipher the data stream.

However, York-Smith does teach a system and method of a client comprising:

a key extractor for extracting an encryption key steganographically hidden in at least one first unit in the data stream received from the server such that steganographic information is needed by the client to determine the encryption key [Fig. 6, step 630]; and

a decoder coupled to the key extractor and the descrambler for reassembling the data stream such that all of the units of the data stream are needed to decipher the data stream [Fig. 6, step 640, also refer to col. 5, lines27 through col. 6, line 15 for further explanation].

It would have been obvious to one of ordinary skill in the art at the time The invention was made to modify REITMEIER et al. to include the key extractor and the decoder of York-Smith. Namely, inserting the key extractor and the decoder in the "subscriber side equipment " of Figure 1 [REITMEIER et al., page 3, paragraph 0035]. One of ordinary skill in the art would have been motivated to modify REITMEIER et al. as above for the purpose of providing a higher level of secure to encrypted data being transmitted over an unsecured transmission line.

Referring to claims 9, 15 and 27, REITMEIER et al. teach the system as recited in claims 8 ,14 and 26, wherein the data stream includes a transmission order which alternates between first units and second units [page 3, paragraph 0034].

Referring to claim 10, REITMEIER et al. as modified teach hiding the encryption key is also steganographically hidden in the at least one second unit [col. 6, lines 6-15].

Referring to claims 11, 17 and 29, REITMEIER et al. as modified by York-Smith teach at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key [York-Smith , col. 3, line 65 through col. 4, lines 22].

Referring to claims 12, 18 and 30, REITMEIER et al. teach a transmission link including the Internet [page 3, paragraph 0033].

Referring to claims 13, 19 and 31, REITMEIER et al. teach at least one of the client and the server include a memory storage device [page 3, paragraph 0035].

Referring to claims 16, 22, and 28, REITMEIER et al. as modified teach the step of steganographically embedding portions of the encryption key in the at least one first unit [York-Smith, col. 3, line 65 through col. 4, lines 22].

In regards to claims 32 and 33, the claim limitations recite a storage medium having instructions to execute the method of claims 1 and 14, therefore the same rejection applies.

Conclusion

Prior arts made of record, not relied upon:

US Patent 5, 613, 004 is directed to an apparatus and method for encoding and decoding additional information into a stream of digitized samples in an integral manner. The information is encoded using special keys. The information is contained in the samples, not prepended or appended to the sample stream. The method makes it extremely difficult to find the information in the samples if the proper keys are not possessed by the decoder. The method does not cause a significant degradation to the sample stream. The method is used to establish ownership of copyrighted digital multimedia content and provide a disincentive to piracy of such material.

US Pub. No. 2002/0152378 discloses a server and a computer are connected to a network. User data may be used to establish a state between a server and a user operating the computer. Key-based secure network user states includes encrypting user data with a cryptographic key; embedding, into the encrypted user data, the cryptographic key or reference data associated with the cryptographic key; storing the encrypted user data with embedded key data in a cookie; and sending the cookie to a computer; such that subsequently, a secure state between the server and the user is established by receiving the cookie from the computer; extracting, from the cookie, the encrypted user data and embedded key data; decrypting, using said key data, the encrypted user data; and establishing the secure state between the server and the user based on the decrypted user data. Key data is the cryptographic key or reference data for obtaining the cryptographic key.

US Pub. No. 20010036271 is directed to a system and method for use in a communication network that communicates with a plurality of digital content servers to provide selected digital data files, including video and audio files, for download to a subscriber device. A segmentation controller is provided for dividing the selected into segments. An encryption controller is provided for compressing and encrypting each of the segments with a selected one of a plurality of encryption keys. The segments are then transmitted at or above the average bandwidth of the communication network to a subscriber device. A copy of the decryption keys are transmitted to the subscriber device to enable playback of the selected file only with a current verification of the subscriber device.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T.A.

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

Gilberto

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100